



UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

BC8

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
-----------------	-------------	----------------------	---------------------

09/294,956 04/20/99 COX

I 12558

WM31/0620

PAUL J ESATTO
SCULLY SCOTT MURPHY & PRESSER
400 GARDEN CITY PLAZA
GARDEN CITY NY 11530

EXAMINER

DI LORENZO, A

ART UNIT

PAPER NUMBER

2131

13

DATE MAILED:

06/20/01

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

Office Action Summary

Application No.

09/294,956

Applicant(s)

COX ET AL.

Examiner

Anthony DiLorenzo

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136 (a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 15 March 2001.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-3, 5-16, 18-41, 47-49, 51-62, 64-87, and 108-134 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-3, 5-16, 18-41, 47-49, 51-62, 64-87, and 108-134 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claims _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are objected to by the Examiner.
- 11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

Attachment(s)

- 15) ☒ Notice of References Cited (PTO-892)
- 16) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 17) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____
- 18) ☐ Interview Summary (PTO-413) Paper No(s) _____
- 19) ☐ Notice of Informal Patent Application (PTO-152)
- 20) ☐ Other:

Art Unit: 2131

DETAILED ACTION

This Office Action is written in response to the appeal brief filed on 3/15/01 in the United States Patent and Trademark Office regarding utility patent application serial no. 09/294956. The
5 finality of the previous office action is withdrawn and prosecution on the merits is re-opened. Claims 1-3, 5-16, 18-41, 47-49, 51-62, 64-87, and 108-134 have been examined on the merits in light of the presented responses.

The appropriate sections of Title 35 of the U.S. Code not appearing in this communication have
10 been cited in a previous office action.

Objections

37 CFR § 1.75 states:

- 15 c) One or more claims may be presented in dependent form, referring back to and **further limiting** another claim or claims in the same application.

(emphasis added)

20 35 USC § 112, fourth paragraph, states:

...a claim in dependent form shall contain a reference to a claim previously set forth and then **specify a further limitation** of the subject matter claimed.

25 Claims 23 and 69 are objected to under 37 CFR § 1.75 (c) and 35 USC § 112, fourth paragraph, for failing to further limit the subject matter of claims 1 and 47, from which they respectively depend. Claims 1 and 47 already contains the limitation wherein the associated data contains an identifier of a public key needed to decrypt the signature.

Claim Rejections

30 Claim rejections are detailed according to each applicable section of Title 35 of the U. S. Code and to each claim below. Rejections of dependent claims necessarily incorporate the rejections of the base claim and any intervening claims. Information contained in rejections of non-related
35 claims may also be incorporated by explicit reference to them. Similar claims are grouped together.

• Under 35 USC § 102

• • New

40 **Claims 117 and 124 are rejected under 35 U.S.C. 102(b)** as being anticipated by Barton ('997).

Barton discloses in column 4, lines 15-20, embedding a digital signature of digital data into that data by inserting the signature into predetermined bit positions of the digital data. In column 6,

Art Unit: 2131

lines 62-65, Barton discloses excluding the predetermined bits from the signature, citing that they will change when the signature is inserted into those bits. The invention of Barton is suitable for signing digital audio, video, and image data (col. 1 line 5).

5 Barton also discloses in column 3, lines 23-30, 45-51 and 58-61, that additional data associated with the digital data, such as a serial number or other identifying information, is also embedded into the digital data and signed. The claim 94 and 98 limitations of receiving data from an external source are also satisfied inherently by Barton. That reference states in column 3, lines 30-47, that embedded authentication data may identify the owner of the digital data. A computer
10 program/apparatus that performs the method could not by its nature know the identity of the owner of the digital data. Therefore, that information would have to be supplied by an external source.

15 Barton discloses the use of public key cryptography, embodied specifically as the RSA algorithm, to encrypt the embedded bitstring, which includes the signature (col. 6, ll. 14-24). In column 7, lines 1-5 Barton discloses that additional data indicating the signature calculation technique may be added to the data to be embedded. Therefore, the associated data contains at least two fields—the identifying information noted above, and the signature calculation
20 technique.

• Under 35 USC § 103

• • Withdrawn

The following rejections are withdrawn:

25 Claims 1-3, 5-16, 18-26, 33-37, 47-49, 51-62, 64-72, 79-83, 117-121, 124-128, and 130-133 under 35 U.S.C. 103(a) as being unpatentable over Barton ('997) in view of Applied Cryptography, by Bruce Schneier.

30 Claims 27-32 and 73-78 under 35 U.S.C. 103(a) as being unpatentable over Barton in view Schneier, and further in view of Conner et al. ('393).

Claims 38-41, 84-87, 108-116, 122, 123, 129, and 134 under 35 U.S.C. 103(a) as being unpatentable over Barton in view of Schneier, and further in view of Bramall ('101).

35 • • New

Claims 1, 3, 5, 6-16, 18-26, 33, 47, 49, 51, 52, 53-55, 56, 57, 58-62, 64-72, 79, 118, 119, 120, 125-127 and 130-133 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barton ('997) in view of Arnold ('172).

40 Claims 1, 3, 22, 23, 25, 47, 49, 68, 69, 71, 118, and 125:

Barton discloses in column 4, lines 15-20, embedding a digital signature of digital data into that data by inserting the signature into predetermined bit positions of the digital data. In column 6, lines 62-65, Barton discloses excluding the predetermined bits from the signature, citing that

Art Unit: 2131

they will change when the signature is inserted into those bits. The invention of Barton is suitable for signing digital audio, video, and image data (col. 1 line 5).

5 Barton also discloses in column 3, lines 23-30, 45-51 and 58-61, that additional data associated with the digital data, such as a serial number or other identifying information, is also embedded into the digital data and signed. The claim 94 and 98 limitations of receiving data from an external source are also satisfied inherently by Barton. That reference states in column 3, lines 30-47, that embedded authentication data may identify the owner of the digital data. A computer
10 program/apparatus that performs the method could not by its nature know the identity of the owner of the digital data. Therefore, that information would have to be supplied by an external source.

15 Barton discloses the use of public key cryptography, embodied specifically as the RSA algorithm, to encrypt the embedded bitstring, which includes the signature (col. 6, ll. 14-24). In column 7, lines 1-5 Barton discloses that additional data indicating the signature calculation technique may be added to the data to be embedded. Therefore, the associated data contains at least two fields—the identifying information noted above, and the signature calculation technique. Barton does not specifically disclose inclusion of data identifying a public key needed to decrypt the signature.

20 Examiner contends that this feature does not make the claims patentable over the prior art, particularly when the invention of Barton is considered in light of the teachings of Arnold. Arnold discloses an apparatus and method for establishing cryptographic links between elements of a system. The vector for establishing the cryptographic links is a public key cryptosystem
25 used to verify the authenticity of a sender of a public/private key pair to a secure chip in an operational unit of the system. These cryptographic units comprise a master key station (MKS), an MKS registration station (MKS-RS), an MKS personalization station (MKS-PS) and a personalization station (PS) (col. 3, ll. 55-65). When establishing a secure communication link between two operational units, each of the operational units will authenticate the other
30 operational unit by verifying the content and source of each of the authentication certificates in the respective chains. The MKS personalizes the secure chips for the PS, the MKS-PS and the MKS-RS. During personalization, a personalizing unit, such as the MKS, provides the secure chip with a public/private signature key pair, designated the SC public signature key and the SC private signature key. The personalizing unit also provides the secure chip with an
35 authentication certificate. An authentication certificate generally contains the SC public signature key and a message indicating the functions that the secure chip has been authorized to perform by the personalizing unit. Finally, the certificate is also signed by the personalizing unit. Various embodiments of the authentication certificates of Arnold are detailed in the appendices, which span columns 35-39 of the patent. Each appendix shows the feature of including in the
40 certificate an identifier public key needed to decrypt the signature on the certificate. Particular attention is directed to appendix A1, col. 35, which clearly shows a "Signature Block" as part of the authentication certificate. Part of the Signature Block includes a "Public Signature Key ID (=MKS Public Signature Key)." Further attention is directed towards col. 38, lines 40 and 60, which define the terms Key ID and Public Signature Key. The disclosure of Arnold clearly

Art Unit: 2131

teaches that it is known in the cryptographic arts to include, along with a public key signature of data, an identifier of the public key needed to decrypt and verify that signature.

5 The person of ordinary skill in cryptography would be motivated to include the Arnold feature of including an identifier of a public key needed to decrypt the signature as part of Barton's existing feature of embedding additional data indicating the signature calculation technique so that a user of the system would be able to more easily find the key required to verify the signature. The person of ordinary skill would recognize that the public key needed to decrypt the signature is an integral part of the signature calculation technique.

10 All independent claim rejections under Barton/Arnold are based on the above combination of references.

Claims 5 and 51:

15 Examiner asserts that in the invention of Barton it would be obvious to insert the additional data into bits of the digital data other than the predetermined bits, since the predetermined bits are already designated for receiving the signature. Any bits residing in the predetermined positions would be overwritten and lost if this were not the case, resulting in an invalid signature.

20 Claims 6 and 52:

Barton discloses in column 7, lines 31-42, that the digital data is divided into blocks (or samples), and that the signature data may be embedded into the least significant bits of a block. Examiner maintains official notice that conceptualizing the least significant bits of an image as an LSB plane is old and well known in the art, and may be applied to any image/video/audio data that is divided into blocks (samples).

Claims 7-9, 12-14, 53-55, and 58-60:

30 Examiner maintains official notice of the following as being old and well-known in the art: a) sampling image data as pixels, b) sampling video data as a particular image position at a particular time (a spatial temporal sample), and c) sampling audio data as a time sample. Since the invention of Barton has been established above to be suited for signing audio/image/video data, and that data is divided into blocks, it would be obvious to use the appropriate sample as the block-type each type of data.

35 Claims 10 and 56:

In the previously cited column 7, lines 31-42, of Barton, all of the embedded data is inserted into the least significant bits, including the signature data and the associated data (see also col. 7, lines 1-5).

40 Claims 11, 15, 16, 57, 61, and 62:

Column 8, lines 31-61, describes transforming a spatially-described image into a frequency-described image, and partitioning the frequency domain into two sections, using Huffman encoding, which takes into account high vs. low frequency components. The predetermined bits are selected from the "least significant bit of a number of the variable length codes in the image."

Art Unit: 2131

Claims 18-20 and 64-66:

Barton discloses that the embedded data may indicate an author of the data (col. 2, ll. 56-60).

- 5 Barton discloses in column 3, lines 31-47, that the associated data may be used to prove ownership of an image by the organization that produced it. From this disclosure, it would be obvious to the person of ordinary skill in data authentication that the associated data may identify any one of a source, owner, or photographer of the digital data.

- 10 Claims 21 and 67: Barton discloses adding an error correction code as a field of the associated data after the other parts of the associated data have been encrypted. Therefore the error encryption code of Barton comprises an unencrypted portion of the associated data (col. 7, lines 25-30).

Claims 24, 70, 119, and 126:

- 15 Barton discloses including an identifier of the source as the embedded information. It is reasonable to expect that the source would also create the signature of the data. This creates the claimed situation, in which an identifier of an owner of the private key is included with the associated data. Further, Arnold also discloses in Appendix A1 an Authorization Block which includes an Authorized ID, which identifies an authorized party that owns the public signing key
20 (col. 35, ll. 15-16 and col. 37, ll. 54-62). Motivation to combine this feature with Barton is the same as above: so that a user of the system would be able to more easily find the key required to verify the signature.

Claims 26, 72, 120, 127, and 130-133:

- 25 The examiner maintains official notice of the following methods of receiving data as being well-known in the art: Global Positioning Satellite transmissions, radio frequency transmissions received by antennae, and internet transmissions received via a networked computer. These methods of importing external data are all within the realm of knowledge of the person of ordinary skill and would be obvious to include in the invention of Barton since external data, at
30 least for the purpose of identifying the meta-data disclosed in column 2, ll. 56-60 of Barton, must be imported.

Claims 33 and 79:

- 35 The rejection of claims 6 and 52 above is incorporated. Barton does not disclose inserting the additional data before signing. In the Barton reference, the additional data is concatenated to the signature, then both are embedded. However, examiner maintains official notice that it would be within the realm of knowledge of the person of ordinary skill in cryptography to include the additional data with the original digital data before signing, so that the signature would encompass both entities. This would increase the security of the additional data. In column 3,
40 line 48, through column 4, line 8, Barton provides motivation for including this feature in the invention of that reference. Barton states that the embedded meta-data (additional data) should be secured by a digital signature.

Art Unit: 2131

Claims 2, 34-37, 48, 80-83, 121, and 128 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barton ('997) in view of Arnold ('172), as applied above, and further in view of Schneier.

5 Claims 2 and 48:

Barton discloses as previously discussed. Barton fails to disclose the use of a hash function signing method. Schneier discloses the well-known method of creating digital signatures using hash functions on page 38, wherein a sender hashes a digital document and encrypts the hash value, thereby creating a signature of the digital document. Since this is a well-known and accepted signing method, it would be within the realm of knowledge of the cryptographer of ordinary skill to implement this method in the invention of Barton. It would be obvious to exclude the predetermined bits from the hash since the hash forms the signature and Barton discloses that the signature should exclude the predetermined bits. Including those bits would significantly change the hash value. If the signature of Barton was then substituted for the predetermined bits (after the hash value had been obtained with the predetermined bits included), that valid signature would always be construed as a forgery because the verification re-hash of the document (created from the copy in which the predetermined bits were overwritten by the signature) would always be different from the original hash value.

20 Claims 34-37, 80-83, 121, and 128:

Barton and Arnold do not disclose time stamping of the digital document to be authenticated. Schneier discloses the well-known authentication method of time stamping on pages 38, 59, and 75-76. A particular protocol is described on page 76 ("Improved Arbitrated Protocol") in which time data is appended to a hash value of the document that is to be time stamped. The time data is signed along with the hash value, making the time data authentic. Schneier does not disclose the steps of claim 104 verbatim, but makes them obvious to the cryptographer of ordinary skill. Schneier states on page 59 that timestamps require a secure and accurate system clock. In light of this, the cryptographer of ordinary skill would be motivated to use a tamper resistant chip containing a clock in order to provide accurate time data, in order to obtain the advantages associated with tamper resistant hardware, as would be within the realm of knowledge of the person of ordinary skill. The step of outputting the signature and time data from the clock to the time stamping circuit would be an obvious step to take in any time-stamping method using a secure clock. A circuit would be necessary to concatenate the time and hash data present in the Schneier reference.

35 **Claims 38-41, 84-87, 108-116, 122, 123, 129, and 134 under 35 U.S.C. 103(a)** as being unpatentable over Barton in view of Arnold, as applied above, and further in view of Bramall ('101).

40 Claims 38, 84, 108-110, 112, 115, and 122:

Barton and Arnold fail to disclose recognizing an authorized user of digital equipment and inserting an identifier thereof into the digital data. Bramall discloses a security system for data handling equipment wherein a pre-authorized user of digital image data generating equipment is recognized by the equipment. The data processed by that user is merged with an identifier of the

Art Unit: 2131

user and recorded on a digital storage means. See Bramall column 2, line 58 through column 3, line 20. The person of ordinary skill in cryptography would be motivated to include the user recognition/recording properties of Bramall in the invention of Barton. Motivation for this inclusion exists in both Bramall and Barton. One of the purposes of Bramall's invention is to identify the user who processed a particular digital record. Barton states on column 3 that a function of embedded authentication data is to detect illegal copying. A digital data generation device that records each user's identity could be an effective deterrent against the production of illegal copies of digital property. The motivation is to increase security in the above referenced manner.

Claims 39, 85, 113:

The primary reference (Barton) discloses signing of the digital data using public key cryptography. Since the intent of Barton's invention is to sign the data to prove ownership, and the obviousness of recognizing and identifying the owner of the data has been established as per Bramall, the person of ordinary skill would be motivated associate a key with a corresponding identity in memory in order to prevent malicious users from making false associations manually.

Claims 40, 86, 114, 123, 129, and 134:

Examiner maintains official notice that fingerprint recognition is a well known form of identification that falls under the general topic of biometrics, and would be obvious to use to identify the user of Bramall to gain the advantages associated with biometrics. Exemplary advantages are that biometrics are not easily forgeable and cannot be lost by users.

Claims 41, 87, 111:

Examiner maintains official notice that a name is a well-known form of identifier and would be obvious to use as the identification in the invention of Bramall. Motivation includes the fact that records of the data are stored on a CD-ROM and may be subject to review by a human operator, whom would most likely find it more comfortable to search through names rather than other forms of identification, such as an arbitrary number.

Claim 116:

Because the invention of Barton is specifically intended to process digital image, video and audio data, it would be obvious to use a digital image generation device to generate a digital image. Examiner maintains official notice that scanners, digital cameras, and digital video cameras are well known in the art of digital image generation and it would be well within the knowledge of the person of ordinary skill to use these devices.

Claims 27-32 and 73-78 under 35 U.S.C. 103(a) as being unpatentable over Barton in view Arnold, as applied above, and further in view of Conner et al. ('393).

Claims 27, 30, 73, and 76:

The cryptographer of ordinary skill is assumed to have within his/her realm of knowledge that most types of compression result in lost data (general computer knowledge), and that a digital signature of the type disclosed in Schneier and applied above will be considered a forgery if an

Art Unit: 2131

attempt is made to verify data from which any bits have been lost, as is the case when a data undergoes lossy compression. For example, if a bitmap image is signed and then compressed under JPEG compression, the resulting JPEG image, even if decompressed, will not contain the same data as the original bitmap image. Therefore, when the JPEG image (compressed or decompressed) is hashed, that hash value would not agree with the decrypted signature that was generated from the original bitmap. Given this knowledge, it would be obvious to the cryptographer of ordinary skill to sign the set of data that is to be verified, and not prior forms of the data. The claims further specify that the signature is inserted into the header of the compressed digital data. Conner et al. disclose the feature of inserting a digital signature into a header of the data that it authenticates (fig. 8A element 104 and col. 9, lines 3-15). It would be obvious to the cryptographer of ordinary skill to use this feature in the combination of Barton and Schneier if that data were to be compressed, because the signature could not be inserted into the compressed data for lack of available bits after the compression: it is well-known to attach a signature to its associated data, and headers are well-known places for inserting information about data.

Claims 28, 29, 31, 32, 74, 75, 77, and 78:

Barton discloses the use of JPEG and MPEG compression in column 8 line 30 through column 9 line 45.

Support for Official Notice

The following references are provided to support the holding of certain features of the prior art as well known.

1. Coles '679 demonstrates that it is well known to receive a global positioning satellite transmission by a digital image generation device. See claim 8 and col. 2, ll. 47-60.
2. Chou et al. '648 demonstrates the ubiquitous and widespread knowledge of fingerprint recognition as a means for identifying users of systems. See entire reference, especially col. 3, ll. 57-66.

Response to Remarks

Applicant's points of traversal were carefully considered. The new rejections above have been applied in order to more fully delineate the prior art. In particular, the Arnold reference is newly cited in the rejections under section 103(a), and discloses as detailed above. Applicant's arguments are considered moot in view of the new grounds of rejection.

Art Unit: 2131

Conclusion

The following prior art made of record but not previously cited is considered pertinent to the applicant's disclosure:


- 5 1. Haber '954 discloses secure times-stamping of digital documents by a third party.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Anthony DiLorenzo, whose telephone number is (703) 306-5617. If the examiner is not available, a voice mail greeting will indicate when the examiner will return to the office. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Official fax number: (703) 308-9051

Unofficial fax number: (703) 305-0040

15 Anthony DiLorenzo
Assistant Examiner
Art Unit 2131
(703) 306-5617


Gail Hayes
Primary Examiner
Art Unit 2131
(703) 305-9711

20 June 18, 2001

AD
6/18/01